明 細 書

暗号化記録装置および方法

技術分野

[0001] 本発明は、MPEGストリームなどの符号化データを暗号化して記録する暗号化記録装置および方法に関するものである。

背景技術

[0002] 近年、マルチメディア技術の進展に伴いディジタル映像データを効率よく記録、再生する技術の開発が進められている。ディジタル映像データ等を記録する際には、著作権保護の観点から所定の暗号化を行って記録することが望まれる場合が多い。この暗号化は、データの安全性を確保するためデータの解読が困難なものが望まれる。例えば、データの解読を困難にする暗号化のひとつとして、1つのコンテンツを複数の領域に分け、この領域毎に暗号化用の鍵を変更して暗号化する方法がある。一方、暗号化されたディジタル映像データ等を再生する際にはスムーズな再生を行うため効率よく復号化してスムーズな画面表示を行うことが望まれる。

[0003] 特許文献1に記載のディジタル信号記録装置は、ディジタル信号の記録時には、鍵情報に所定の演算を施して得られた鍵でディジタル信号を暗号化し、暗号化したデータを鍵情報とともに記録媒体に記録している。そして、ディジタル信号の再生時には、記録媒体から再生した鍵情報に所定の演算を施して得られた鍵で再生した暗号化データを復号化して出力している。これによって、記録媒体上の鍵情報を得ても再生時に所定の演算を施さなければ鍵を得ることができないようにしている。また、この特許文献1には、暗号鍵を一定間隔で変更することで、データの安全性を高めることが開示されている。

[0004] 特許文献1:国際公開第00／52690号パンフレット

発明の開示

発明が解決しようとする課題

[0005] しかしながら、上記従来の技術によれば、暗号鍵を一定間隔で変更しながらディジタル信号を暗号化している。このため、GOP(Group of picture)内の1つのIピクチ

ャを暗号化している時に暗号鍵の変更が行われる場合がある。このような場合、1つのIピクチャが複数の暗号鍵で暗号化されることとなり、ディジタル信号を再生する際には1つのIピクチャに複数の復号鍵を要することとなる。1つのIピクチャを複数の復号鍵で復号化する場合、例えば早送り再生、サーチ等の特殊再生を行う際に、復号鍵の変更処理が介入するためスムーズな映像表示ができないといった問題があった。本発明が解決しようとする課題は上記した問題が一例として挙げられる。

[0006] 本発明は、上記に鑑みてなされたものであって、早送り再生、サーチ等の特殊再生を行う際に、復号鍵の変更処理が介入しないスムーズな映像表示をなし得る暗号化記録装置および方法を得ることを目的とする。

課題を解決するための手段

[0007] 上述した課題を解決し、目的を達成するために、請求項1に記載の発明は、フレーム内符号化画像を少なくとも含む符号化単位により構成される符号化データが入力される入力手段と、前記符号化データを所定の暗号化単位で暗号化するとともに、一又は複数の暗号化単位毎に暗号鍵を変更しつつ前記符号化データを暗号化する暗号化処理手段と、前記暗号化された符号化データを記録媒体に記録する記録手段とを備えた暗号化記録装置において、前記暗号化処理手段は前記一つのフレーム内符号化画像を暗号化する途中で暗号鍵が変更されないよう少なくとも一つのフレーム内符号化画像を単一の暗号化鍵で暗号化すること、を特徴とする。

[0008] また、請求項6に記載の発明は、フレーム内符号化画像を少なくとも含む符号化単位により構成される符号化データを、暗号鍵を変更しながら所定の暗号化単位で暗号化して記録する暗号化記録方法において、前記一つのフレーム内符号化画像を暗号化する途中で暗号鍵が変更されないよう少なくとも一つのフレーム内符号化画像を単一の暗号化鍵で暗号化することを特徴とする。

図面の簡単な説明

[0009] [図1]図1は、実施例1にかかる暗号化記録装置の構成を説明するためのブロック図である。

[図2]図2は、記憶手段に記憶される情報を示す図である。

[図3]図3は、記録媒体内に記録される情報を示す図である。

[図4]図4は、CBCとピクチャの関係を説明するための図である。

[図5]図5は、実施例1にかかる暗号化記録装置の暗号化から記録までの処理手順を示すフローチャートである。

[図6]図6は、実施例2にかかる暗号化記録装置の構成を説明するためのブロック図である。

[図7]図7は、CBCとGOPの関係を説明するための図である。

[図8]図8は、NULLパケットを挿入する手順を示すフローチャートである。

符号の説明

[0010] 10 暗号化記録装置

15 暗号化記録装置

20 情報供給手段

21 鍵変更禁止フラグ

30 暗号化手段

31 CBCカウンタ

32 鍵生成手段

40 記録手段

50 記録媒体

60 CPU

62 記憶手段

70 暗号鍵供給手段

80 暗号鍵生成手段

100 暗号化処理手段

発明を実施するための最良の形態

[0011] 以下に、本発明にかかる暗号化記録装置および方法の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。以下では、本発明の暗号化記録装置の概略と特徴を実施の形態として説明し、その後に暗号化記録装置に関する実施例を説明する。

[0012] [実施の形態]

本実施の形態において、暗号処理の対象としてのコンテンツは、MPEG−TS(Motion Picture Expert Group−Transport Stream)等の符号化データである。また、コンテンツは、MPEGにおけるIピクチャのように自フレーム内の情報のみで符号化されたフレーム内符号化画像とその他の符号化画像を含んでいる。その他の画像としては、例えば、MPEGにおけるPピクチャのような時間的に過去に位置するピクチャから予測して作られるフレーム間順方向予測符号化画像および／またはBピクチャのような時間的に前後に位置するピクチャから予測して作られるフレーム間双方向予測符号化画像などが想定される。MPEGでは、Iピクチャ、PピクチャおよびBピクチャの組み合わせによって符号化単位であるGOP(Group of picture)が構成される。GOPには各種の方式があるが、1つのGOPには、少なくとも1つのIピクチャが必ず存在する。

[0013] 一方、暗号化方式としては、DES(Data Encryption Standard)、3DES、AES(Advanced Encryption Standard)などのように、所定のデータ長(64、128、256バイト)毎に暗号化する方式を採用し、さらに、平文の保護の観点から暗号ブロック連鎖方式(Cipher Block chaining:CBC)を採用する。また、暗号鍵は、1ー複数のCBCブロック単位に変更される。すなわち、本実施の形態においては、MPEG−TSなどの符号化データを所定の暗号化単位毎に暗号化するとともに暗号鍵を1ー複数の暗号化単位毎に変更するような暗号化処理が行われる。

[0014] このような符号化データを所定の暗号化単位毎に暗号化して記録メディアに記録するとき、符号化データで意味のある区間と、暗号化単位の長さとの間には、何の相関性もない。符号化データで意味のある区間とは、MPEGの場合は、ピクチャやGOPの切れ目のことを指す。

[0015] したがって、一定期間毎に暗号鍵を変更する手法では、1つのフレーム内符号化画像(MPEGでは、Iピクチャ)を暗号化している時に暗号鍵の変更が行われる場合がある。すなわち、1つのフレーム内符号化画像が複数の暗号鍵で暗号化されることとなり、この箇所を再生する際には、複数の復号鍵を要することとなる。早送り再生、サーチ等では、フレーム内符号化画像(Iピクチャ)のみを抽出して再生するが、1つのフレーム内符号化画像再生中に、復号鍵の変更処理が介入すると、スムーズな映

像表示ができない。

[0016] そこで、本実施の形態においては、少なくとも1つのフレーム内符号化画像を含む符号化画像を同一の暗号鍵をもって暗号化するようにしている。

[0017] 例えば、符号化データを暗号化する際の暗号鍵を変更するタイミングである暗号鍵変更タイミングがフレーム内符号化画像を暗号化する途中となる場合は、暗号鍵変更タイミングがフレーム内符号化画像を暗号化する途中とならないよう前記変更タイミングを遅延させることにより、フレーム内符号化画像を同一の暗号鍵で暗号化したり、あるいは暗号鍵変更タイミングがフレーム内符号化画像を含む前記符号化単位を暗号化する途中となる場合は、暗号鍵変更タイミングが前記符号化単位を暗号化する途中とならないようNULLパケット、ランダムデータなどの意味をもたない情報を挿入することにより、少なくとも1つのフレーム内符号化画像を含む符号化画像を単一の暗号鍵をもって暗号化する。

[0018] このように、実施の形態においては、暗号鍵を変更するタイミングがフレーム内符号化画像の途中とならないようにしているので、少なくとも1つのフレーム内符号化画像を同一の暗号鍵で暗号化することができ、これにより少なくとも1つのフレーム内符号化画像を同一の復号鍵で復号化することができる。したがって、早送り再生やサーチ時にスムーズな映像表示が可能となる。

[0019] [実施例1]

図1は、本発明の実施例1にかかる暗号化記録装置の構成を説明するためのブロック図である。iVDR(Intelligent Video Digital Recorder)などに適用される暗号化記録装置10は、MPEG—TS等の符号化データをリアルタイムに暗号化して記録するものであり、情報供給手段20、暗号化処理手段100、記録手段40、制御手段としてのCPU(Central Processing Unit)60および記憶手段(RAM)62を備えている。暗号化処理手段100は、暗号化手段30、暗号鍵供給手段70および暗号鍵生成手段80を備えている。また、暗号化記録装置10は記録媒体50と接続されている。

[0020] 情報供給手段20は、外部から符号化データが入力される入力手段であり、暗号化手段30、暗号鍵供給手段70、CPU60に接続されている。情報供給手段20は、CPU60からの制御信号によって動作の開始や停止が制御されており、外部入力される

パーシャルTS(Transport Stream)信号を、暗号化手段30において暗号化されるデータサイズ毎にバッファリングしながら所定のタイミングで暗号化手段30に供給する。パーシャルTS信号は、MPEG—TS信号のうち録画再生に必要な情報が抽出されたものである。

[0021] また、情報供給手段20は、入力されたパーシャルTS信号に基づいて鍵変更を禁止するか否かを判定するデータ識別手段(図示せず)を有している。データ識別手段は、その判定結果に応じて、暗号鍵の変更を禁止する否かを識別させる識別フラグとしての鍵変更禁止フラグの状態を変化させる。鍵変更禁止フラグは、鍵変更を禁止する場合は、「1」とし、鍵変更を許可する場合は、「0」とする。

[0022] ここで、MPEGでエンコード(符号化)された映像データは188バイトあるいは192バイトのように所定のサイズでパケット化されている。MPEGでのエンコードでは、映像データなどに応じて情報圧縮率が異なり、映像データはデータ長が不定長のIピクチャ、Bピクチャ、Pピクチャ等によって構成されている。

[0023] Iピクチャは、前述したように、自フレーム内の情報のみで符号化されたフレーム内符号化画像であり、時間的に前後する他の画面の相関情報を用いない。Iピクチャは映像データの中に一定周期で配置されている。Pピクチャは、時間的に過去に位置するIピクチャやPピクチャから予測して作られるフレーム間順方向予測符号化画像である。Bピクチャは、時間的に前後に位置するIピクチャやPピクチャから予測して作られるフレーム間双方向予測符号化画像である。

[0024] また、これらIピクチャ、PピクチャおよびBピクチャの組み合わせによってGOP(Group of picture)が構成される。GOPには、各種の方式があり、例えば、IBBPBBPBBPBBPBBの15ピクチャ(フレーム)で1つのGOPを構成したり、あるいはIBBPBBPBBPBBPBBPBBの18ピクチャ(フレーム)で1つのGOPを構成したりする。1つのGOPには、少なくとも1つのIピクチャが必ず存在する。

[0025] 情報供給手段20は、暗号化手段30で暗号化されるピクチャがIピクチャであるか否かの判断を行うために、入力されたパーシャルTS信号中のIピクチャを検出し、Iピクチャを検出している期間中は、鍵変更禁止フラグを「1」とし、Iピクチャを検出していない期間中は、鍵変更禁止フラグを「0」とする。情報供給手段20は、例えば、Iピクチャ

の先頭、またはそれに類するシーケンスヘッダコード(SHC)、GOPヘッダ等を検出した時点から他のBピクチャやPピクチャの先頭を検出した時点までの間を、Iピクチャの検出期間とし、このIピクチャの検出期間中は、鍵変更禁止フラグを「1」とし、Iピクチャの検出期間以外の期間は、鍵変更禁止フラグを「0」とする。この鍵変更禁止フラグは、暗号鍵供給手段70で参照することができる。

[0026] 暗号鍵生成手段80は、CPU60から鍵生成通知信号を受信すると、新たな暗号鍵を生成し、生成した暗号鍵を暗号鍵供給手段70に送る。CPU60から暗号鍵生成手段80に送られる鍵生成通知信号は、暗号鍵変更タイミングを示すものであり、タイマやカウンタなどによってその送出時間間隔を設定することで、例えば、一定時間間隔であるいは一定のCBCブロック数毎に鍵生成通知信号が発生される。すなわち、暗号鍵生成手段80では、鍵生成通知信号に応答して異なる暗号鍵を順次生成し、生成した暗号鍵を暗号鍵供給手段70に送る。

[0027] 暗号鍵供給手段70は、暗号鍵生成手段80から入力された暗号鍵を保持し、保持した暗号鍵を、鍵変更禁止フラグの状態に応じて決定したタイミングで暗号化手段30および記憶手段62に出力する。すなわち、暗号鍵供給手段70は、鍵変更禁止フラグが「0」のときには、暗号鍵生成手段80から入力された暗号鍵を即座に暗号化手段30に出力するが、鍵変更禁止フラグが「1」のときには、暗号鍵生成手段80から暗号鍵が入力されても、この時点では暗号鍵を暗号化手段30に出力せず、暗号鍵を保持しておき、鍵変更禁止フラグが「1」から「0」となった時点の後の、最初の暗号化ブロック間の境界位置に対応する時点で暗号鍵を暗号化手段30に出力する。このように、この場合は、暗号鍵供給手段70が暗号化手段30における暗号化の際の鍵変更タイミングを調整している。

[0028] 暗号化手段30は、暗号化単位である暗号化ブロック(CBCブロック)の個数をカウントするCBC(Cipher Block Chaining)カウンタ31を備えており、情報供給手段20、暗号鍵供給手段70、記録手段40およびCPU60と接続されている。暗号化手段30は、暗号鍵供給手段70から入力される暗号鍵を用いて情報供給手段20から入力されるパーシャルTS信号に対し固定長の暗号化ブロック毎に暗号化を行うものであり、暗号化されたパーシャルTS信号(以下暗号化データという)を記録手段40に出力

する。CBCカウンタ31は、暗号化を行ったCBCブロックの個数をカウントするものであり、そのカウント結果をCPU60を介して記憶手段62に出力する。なお、CBCとは、前述したように、現時点の平文に1つ前の暗号文を加え、この加えた結果をDES(Data Encryption Standard)、3DES、AES(Advanced Encryption Standard)等で暗号化する暗号ブロック連鎖方式である。

[0029] 記録手段40は、暗号化手段30から得た暗号化データと、CPU60から得た暗号化データの管理情報(記憶手段62に一時記憶される)を記録媒体50に記録させる。記録媒体50は、ハードディスク,DVDなどの光記録媒体等の記録メディアであり、記録媒体50には、記録手段40から送られる暗号化データおよび暗号化データの管理情報が記録される。

[0030] CPU60は、暗号化記録装置10の各構成要素(情報供給手段20、暗号化手段30、記録手段40、暗号鍵供給手段70、暗号鍵生成手段80)を統括的に制御するとともに、暗号化手段30で暗号化された暗号化データの管理情報を記憶手段62に一時的に記憶する。また、CPU60は、前述した暗号鍵変更タイミング信号としての鍵生成通知信号を、例えば、所定個数のCBCブロック数に対応する一定時間間隔で、暗号鍵生成手段80に出力する。

[0031] つぎに、記憶手段62に記憶される管理情報について説明する。図2は、記憶手段62に記憶される管理情報の具体例を示すものである。管理情報は、鍵適用数Aと鍵適用範囲情報B1ーBn(nは自然数)からなる。鍵適用数Aは、暗号化手段30での暗号化の際に用いた鍵数n、すなわち鍵適用範囲情報B1ーBnの個数を示すものである。鍵適用範囲情報B1ーBnは、鍵情報X、鍵適用開始CBC番号Y、鍵適用CBC数Zからなる。鍵情報Xは、暗号化手段30での暗号化の際に用いた暗号鍵、すなわち暗号鍵生成手段80で生成された暗号鍵を示す情報であり、この暗号鍵が復号化の際の復号鍵となる。

[0032] 鍵適用開始CBC番号Yは、鍵Xの適用が開始されるCBCブロックの番号である。例えば、10番目のCBCブロックから鍵Xが適用される場合、適用開始CBC番号Yは10となる。鍵適用CBC数Zは、鍵Xが適用されるCBCの個数を示すものである。例えば、10番目のCBCブロックから15番目のCBCブロックまで鍵Xが適用される場合、

適用CBC数Zは6となる。

[0033] つぎに、記録媒体50に記録される情報について説明する。図3は、記録媒体50内に記録される情報を示すものある。記録媒体50に書き込まれる情報は、前述した管理情報ファイルと暗号化データから構成されている。

[0034] 管理情報ファイルは、記録媒体50に記録された暗号化データを管理するための情報を含んでおり、記憶手段62に一時記憶される管理情報と同様、鍵適用数A、鍵適用範囲情報B1ーBnを有している。そして、各鍵適用範囲情報B1ーBnは、前記同様、鍵情報X、鍵適用開始CBC番号Y、鍵適用CBC数Zからなっている。記録媒体50に記録される暗号化データは、暗号化手段30で暗号化されたパーシャルTS等の情報である。

[0035] つぎに、CPU60から指令された鍵生成通知信号による暗号鍵変更タイミングを遅延させる方法について説明する。本実施例1においては、Iピクチャ等を抽出して行う早送り再生等をスムーズに行うため、1つのIピクチャが複数の異なる復号鍵で復号されることがないよう、1つのIピクチャは同一の暗号鍵で暗号化する。

[0036] MPEG−TS等を受信しながら記録する場合は、リアルタイム処理であるため、各Iピクチャのデータの長さを予め認識することが困難である。また、ピクチャの間にNULL(ヌル)パケット等を挿入すると元のMPEG−TSのデータに対してどのような影響を与えるかを予測することが困難である。したがって、本実施例1においては、1つのIピクチャが異なる復号鍵で復号されることがないように、鍵変更禁止フラグの状態を参照して、鍵変更を行うタイミングを遅延させるようにしている。

[0037] 図4は、CBCブロックとピクチャの関係を説明するための図である。図4において、暗号化を行うためのCBCブロックは固定長であり、初期段階においては、CPU60から指令される鍵生成通知信号によって、例えば、3個のCBCブロック毎に暗号鍵が変更されるように鍵変更タイミングが設定されているものとする。初期段階においては、図4中、最初の3つのCBCブロック1(CBC1)は同一の第1の暗号鍵で暗号化が行われ、つぎの3つのCBCブロック2(CBC2)が第1の暗号鍵とは異なる第2の暗号鍵で暗号化が行われるように設定され、時点aが初期段階における鍵変更タイミングであったものとする。すなわち、鍵生成通知信号による初期段階の暗号鍵変更タイミン

グでは、時点aに暗号鍵供給手段70から新たな第2の暗号鍵が暗号化手段30に入力され、区間bにあるCBCブロックは初期段階においては、第2の暗号鍵によって暗号化されるCBC2ブロックであったものとする。

[0038] この場合、CPU60から指令される鍵生成通知信号による初期の鍵変更タイミングaは、Iピクチャの途中となる。このため、このままでは、Iピクチャは2種類の暗号鍵で暗号化されてしまう。そこで、実施例1では、1つのIピクチャが異なる暗号鍵を用いて暗号化されることがないよう、鍵変更タイミングを遅らせるようにしている。ここでは、鍵変更タイミングを暗号化単位である1つのCBCブロック分だけ遅らせ、新たな鍵変更タイミングを時点cとしている。

[0039] すなわち、初期段階の鍵変更タイミングである時点aでは、鍵変更禁止フラグが1であるので、暗号鍵供給手段70は、この時点aでは、新たな第2の暗号鍵を暗号化手段30に入力しない。暗号鍵供給手段70では、鍵変更禁止フラグが0となった後の最初のCBCブロックの境界時点cに新たな第2の暗号鍵を暗号化手段30に入力する。したがって、時点aでは、暗号化手段30において鍵変更は行われず、区間bの暗号化ブロックは第1の暗号鍵を用いて暗号化される暗号化ブロックCBC1となる。そして、時点c以降の3つのCBCブロックについては、第2の暗号鍵を用いて暗号化される暗号化ブロックCBC2となっている。

[0040] このようにして、1つのIピクチャはCBC1の暗号化用の鍵のみによって暗号化されることとなる。1つのIピクチャが1つの暗号鍵で暗号化された場合は、1つのIピクチャを1つの復号鍵で復号することが可能となる。なお、図4の場合は、1つのCBC2をCBC1に変更するのみで、1つのIピクチャを同一の暗号鍵を用いて暗号化することができているが、Iピクチャの長さによっては、2個ー複数のCBC2, CBC3をCBC1に変更することもある。

[0041] また、図4の場合は、1つのCBC2をCBC1に変更しているにも係わらず、第2の暗号鍵で暗号化されるCBCブロック(CBC2)の個数を初期段階で設定された3個のままとなるようにしているが、CBC2からCBC1に変更されたCBCブロックの個数分(この場合は1個)だけ、第2の暗号鍵で暗号化されるCBCブロック(CBC2)の個数を減らせるようにしてもよい。その場合、図4におけるCBCブロック(CBC2)の個数は2個

となる。

[0042] つぎに、図5のフローチャートを参照して、図1に示した各構成要素の動作を詳細に説明する。図5は、図1に示した各構成要素のハードフローをソフトウェア的なフローチャートとして表したものである。

[0043] 記録動作が開始されると、記憶手段62、CBCカウンタ31、鍵変更禁止フラグ21をクリアする初期化処理が行われる(ステップS100)。

[0044] つぎに、暗号鍵生成手段80は、第1番目の暗号鍵を生成し、生成した暗号鍵を暗号鍵供給手段70に供給する(ステップS110, S120)。暗号鍵供給手段70は、記録開始時点では、暗号鍵生成手段80から供給された暗号鍵を、無条件にすなわち鍵変更禁止フラグを参照することなく暗号化手段30に即座に出力する。さらに、暗号鍵供給手段70は、暗号鍵生成手段80から供給された暗号鍵を、CPU60に出力する。

[0045] つぎに、暗号化手段30は、暗号鍵生成手段80から供給された暗号鍵を用いた暗号化処理をデータが入力されるまでの間待機するデータ入力待ちの状態となる(ステップS130)。また、記録手段40も、記録すべきデータが入力されるまでの間記録処理を待機するデータ入力待ちの状態となる(ステップS140)。

[0046] つぎに、情報供給手段20は、パーシャルTS信号が入力されると、入力されるパーシャルTS信号中のピクチャ検出動作を開始する(ステップS150)。

[0047] すなわち、情報供給手段20は、パーシャルTS信号が入力されると、入力されたパーシャルTSを所定のデータサイズ毎にバッファリングしながら所定のタイミングで暗号化手段30に供給するとともに、暗号化手段30で暗号化されるピクチャがIピクチャであるか否かの判断を行うため、入力されたパーシャルTS信号中のIピクチャの先頭を検出する(ステップS160)。情報供給手段20は、Iピクチャの先頭、またはそれに類するシーケンスヘッダコード(SHC)、GOPヘッダ等を検出することにより、Iピクチャの先頭を検出する。

[0048] そして、情報供給手段20は、Iピクチャの先頭を検出すると、鍵変更禁止フラグを「0」から「1」に立ち上げる。鍵変更禁止フラグは、他のBピクチャやPピクチャの先頭を検出するまでは、「1」に保持され、他のBピクチャやPピクチャの先頭を検出した地点で(ステップS180)、「0」に立ち下げられる(ステップS190)。このようにして、Iピクチ

ャが検出されている期間中は、鍵変更禁止フラグは「1」に保持され、Iピクチャを検出していない期間中は、鍵変更禁止フラグは「0」とされる。情報供給手段20では、このようなステップS160ーS190の処理を繰り返し実行する。

[0049] 一方、情報供給手段20にパーシャルTS信号が入力されると、その旨が情報供給手段20からCPU60に報告される。これにより、CPU60は、鍵適用数Aの値を＋1し、その＋1した結果（この場合は鍵適用数A＝1）を記憶手段62の鍵適用数Aの記憶エリアに記憶する（ステップS200）。

[0050] さらに、CPU60は、ステップS120の時点において、暗号鍵供給手段70から供給されていた第1番目の暗号鍵を、記憶手段62の鍵情報Xの記憶エリアに記憶する（ステップS210）。さらに、CPU60は、暗号化手段30のCBCカウンタ31のカウント出力を取得し、取得したカウント結果（この場合は、CBCカウンタ31の初期値）を記憶手段62の鍵適用開始CBC番号Yの記憶エリアに記憶しておく（ステップS220）。

[0051] つぎに、暗号鍵生成手段80がCPU60から鍵生成通知信号を受信までの間（ステップS230、No）、暗号化手段30は、情報供給手段20からパーシャルTS信号が入力された時点から、ステップS110において情報供給手段20から入力された第1番目の暗号鍵を用いてCBCブロック単位の暗号化処理を行う。すなわち、暗号化手段30は、情報供給手段20からCBCブロック単位に入力されたパーシャルTS信号を、第1番目の暗号鍵を用いてCBCブロック単位に順次暗号化し、暗号化されたパーシャルTS信号すなわち暗号化データをCBCブロック単位にバッファリングしながら記録手段40に順次出力する（ステップS240）。CBCカウンタ31は、1つのCBCブロックが暗号化されると、そのカウント値を＋1し、そのカウント値をCPU60に出力する（ステップS250）。また、記録手段40は、暗号化手段30から入力された暗号化データを、順次記録媒体50の所要のエリアに順次記録していく（ステップS260）。以上のような暗号化手段30での第1番目の暗号鍵を用いた暗号化処理、CBCカウンタ31のインクリメントおよび記録手段40での記録動作は、CPU60からの鍵生成通知信号が暗号鍵生成手段80に入力されるまで繰り返される。

[0052] その後、CPU60からの鍵生成通知信号が暗号鍵生成手段80に入力されると（ステップS230、Yes）、暗号鍵生成手段80は、第2番目の暗号鍵を生成し、生成した

第2番目の暗号鍵を暗号鍵供給手段70に出力する。暗号鍵供給手段70は入力された第2番目の暗号鍵を保持するとともに、情報供給手段20の鍵変更禁止フラグ21の状態を参照する(ステップS290)。この場合、情報供給手段20の鍵変更禁止フラグ21は「0」であったとする。

[0053] 暗号鍵供給手段70は、鍵変更禁止フラグが「0」であるので(ステップS290、No)、暗号鍵生成手段80から入力された保持している暗号鍵を即座に暗号化手段30およびCPU60に出力する(ステップS330)。CPU60は、この時点でのCBCカウンタ31のカウント値からステップS220で取得した鍵適用開始CBC番号Yの値を減算する演算を行い、この演算結果を鍵適用CBC数Zとして記憶手段62で記憶する(ステップS340)。すなわち、この場合、ステップS340では、ステップS230ーS260を繰り返すことによって行われた第1番目の暗号鍵による暗号化処理での鍵適用CBC数Zが演算される。

[0054] つぎに、CPU60は、鍵適用数Aの値を＋1し、その＋1した結果(この場合は鍵適用数A＝2となる)を記憶手段62の鍵適用数Aの記憶エリアに記憶する(ステップS200)。

[0055] さらに、CPU60は、ステップS330の時点において、暗号鍵供給手段70から供給されていた第2番目の暗号鍵を、記憶手段62の鍵情報Xの記憶エリアに記憶する(ステップS210)。さらに、CPU60は、この時点の暗号化手段30のCBCカウンタ31のカウント出力を取得し、取得したカウント結果を記憶手段62の鍵適用開始CBC番号Yの記憶エリアに記憶しておく(ステップS220)。

[0056] つぎに、暗号鍵生成手段80がCPU60から新たな鍵生成通知信号を受信するまでの間(ステップS230、No)、暗号化手段30は、ステップS330において情報供給手段20から入力された第2番目の暗号鍵を用いてCBCブロック単位の暗号化処理を行う。すなわち、暗号化手段30は、情報供給手段20からCBCブロック単位に入力されたパーシャルTS信号を、第2番目の暗号鍵を用いてCBCブロック単位に順次暗号化し、暗号化データをCBCブロック単位にバッファリングしながら記録手段40に順次出力する(ステップS240)。CBCカウンタ31は、1つのCBCブロックが暗号化されると、そのカウント値を＋1し、そのカウント値をCPU60に出力する(ステップS250)。

また、記録手段40は、暗号化手段30から入力された暗号化データを、順次記録媒体50の所要のエリアに順次記録していく(ステップS260)。以上のような暗号化手段30での第2番目の暗号鍵を用いた暗号化処理、CBCカウンタ31のインクリメントおよび記録手段40での記録動作を、CPU60からの新たな鍵生成通知信号が暗号鍵生成手段80に入力されるまで繰り返す。

[0057] その後、CPU60からの鍵生成通知信号が暗号鍵生成手段80に入力されると(ステップS230、Yes)、暗号鍵生成手段80は、第3番目の暗号鍵を生成し、生成した第3番目の暗号鍵を暗号鍵供給手段70に出力する。暗号鍵供給手段70は入力された第3番目の暗号鍵を保持するとともに、情報供給手段20の鍵変更禁止フラグ21の状態を参照する(ステップS290)。

[0058] この場合、情報供給手段20の鍵変更禁止フラグ21は「1」であったとする。暗号鍵供給手段70は、鍵変更禁止フラグが「1」であるので(ステップS230、Yes)、暗号鍵生成手段80から入力された第3番目の暗号鍵を、この時点では、暗号化手段30に出力しない。そして、暗号鍵供給手段70では、この第3番目の暗号鍵を保持しておき、鍵変更禁止フラグが「1」から「0」となった時点の後の、最初の暗号化ブロック間の境界位置に対応する時点(図4における時点c)で、第3番目の暗号鍵を暗号化手段30に出力する(ステップS330)。

[0059] なお、この場合は、暗号鍵供給手段70は、暗号鍵生成手段80から供給された暗号鍵を即座に暗号化手段30に入力すれば、暗号化手段30ではCBCブロックの境界で暗号鍵が変更されるように各部のタイミング調整が行われている。したがって、暗号鍵供給手段70では、暗号鍵生成手段80から暗号鍵が入力された時点(例えば図4の時点a)後の、1ー複数のCBCブロック分に対応する時間が経過した時点(図4における時点c, 時点d,…)をタイマカウンタなどを用いて順次検出することで、暗号化ブロック間の境界位置を検出し、鍵変更禁止フラグが「1」から「0」となった時点の後に、最初の暗号化ブロック間の境界位置に対応する時点を検出した時点で、第3番目の暗号鍵を暗号化手段30に出力するようにすればよい。

[0060] 上述のように、暗号鍵供給手段70は、鍵変更禁止フラグが「1」である場合、暗号鍵生成手段80から入力された暗号鍵(この場合第3の暗号鍵)を保持し、鍵変更禁止

フラグが「1」から「0」となった時点の後の、最初の暗号化ブロック間の境界位置に対応する時点（図4における時点c）で暗号鍵を暗号化手段30に出力するようにしている。このようにして暗号鍵供給手段70は、新たな暗号鍵（この場合第3の暗号鍵）を暗号化手段30に供給するタイミングを遅延させるようにしている。

[0061] したがって、暗号鍵生成手段80から新たな暗号鍵（この場合第3の暗号鍵）が出力されてから、暗号鍵供給手段70から暗号化手段30に対し暗号鍵（この場合第3の暗号鍵）が供給されるまでの間の期間、すなわち暗号鍵供給手段70による遅延時間の間は、暗号化手段30では、第2の暗号鍵による暗号化が行われることになる。

[0062] すなわち、この遅延時間の間、暗号化手段30は、情報供給手段20からCBCブロック単位に入力されたパーシャルTS信号を、第2番目の暗号鍵を用いてCBCブロック単位に順次暗号化し、暗号化データをCBCブロック単位にバッファリングしながら記録手段40に順次出力する（ステップS300）。CBCカウンタ31は、1つのCBCブロックが暗号化されると、そのカウント値を＋1し、そのカウント値をCPU60に出力する（ステップS310）。また、記録手段40は、暗号化手段30から入力された暗号化データを、順次記録媒体50の所要のエリアに順次記録していく（ステップS320）。

[0063] 以上のような暗号化手段30での第2番目の暗号鍵を用いた暗号化処理、CBCカウンタ31のインクリメント処理および記録手段40での記録動作は、鍵変更禁止フラグが「1」から「0」となるまでは繰り返される。正確には、鍵変更タイミングの変更によって追加される第2番目の暗号鍵を用いた暗号化処理は、鍵変更禁止フラグが「1」から「0」となった後、情報供給手段20から新たな第3番目の鍵が暗号化手段30に供給されるまで、実行される。

[0064] この場合、暗号鍵供給手段70は、前述したように、鍵変更禁止フラグが「1」から「0」となった時点の後の、最初の暗号化ブロック間の境界位置に対応する時点（図4における時点c）で第3の暗号鍵を暗号化手段30およびCPU60に出力する（ステップS330）。

[0065] CPU60は、この時点でのCBCカウンタ31のカウント値からステップS220で取得した鍵適用開始CBC番号Yの値を減算する演算を行い、この演算結果を鍵適用CBC数Zとして記憶手段62で記憶する（ステップS340）。すなわち、この場合、ステップS

340では、ステップS230ーS260の処理の繰り返し、およびステップS300ーS320の処理を実行することによって行われた第2番目の暗号鍵による暗号化処理での鍵適用CBC数Zが演算される。

[0066] つぎに、CPU60は、鍵適用数Aの値を＋1し、その＋1した結果(この場合は鍵適用数A＝3となる)を記憶手段62の鍵適用数Aの記憶エリアに記憶する(ステップS200)。

[0067] さらに、CPU60は、ステップS330の時点において、暗号鍵供給手段70から供給されていた第3番目の暗号鍵を、記憶手段62の鍵情報Xの記憶エリアに記憶する(ステップS210)。さらに、CPU60は、この時点の暗号化手段30のCBCカウンタ31のカウント出力を取得し、取得したカウント結果を記憶手段62の鍵適用開始CBC番号Yの記憶エリアに記憶しておく(ステップS220)。

[0068] つぎに、前述と同様、ステップS230ーS260の処理を繰り返すことにより、暗号化手段30での第3番目の暗号鍵を用いた暗号化処理、CBCカウンタ31のインクリメントおよび記録手段40での記録動作が実行される。

[0069] その後、CPU60からの鍵生成通知信号が暗号鍵生成手段80に入力されると(ステップS230、Yes)、暗号鍵生成手段80は、第4番目の暗号鍵を生成し、生成した第4番目の暗号鍵を暗号鍵供給手段70に出力する。これ以降の動作は、前述と同様であり、情報供給手段20の鍵変更禁止フラグ21の状態に応じて、鍵変更タイミングを変更するか否かが決定され、この決定結果に応じた暗号化処理が実行される。

[0070] このように実施例1によれば、1つのIピクチャの途中で暗号鍵の変更タイミングが発生した場合は、暗号鍵の変更タイミングを遅らせて1つのIピクチャを同一の暗号鍵で暗号化するようにしたので、MPEGーTS等の符号化映像データを受信しながら暗号化して記録媒体に記録するリアルタイム暗号化記録装置において、早送り再生やサーチ時にスムーズな映像表示が可能となる。

[0071] なお、上記実施例1においては、暗号鍵供給手段70が暗号化手段30における暗号化の際の鍵変更タイミングを調整するようにしたが、暗号化手段30において、鍵変更タイミングを調整するようにしてもよい。例えば、暗号化手段30に、新旧2つの暗号鍵を保持するバッファを設ける。暗号鍵供給手段70は、鍵変更禁止フラグ21の状態

識別により、新旧2つの暗号鍵のうちのどちらを使用するかを示す識別信号を暗号化手段30に入力する。暗号化手段30では、CBCブロックの区切りがくるたびに、識別信号を参照して使用すべき暗号鍵を新旧2つの暗号鍵から選択し、選択した暗号鍵を使用して暗号化を行う。また、上記実施例1では、CPU60が暗号鍵を変更するタイミングを指令するようにしたが、暗号化処理手段100自体に暗号鍵変更タイミングを予め設定するようにしてもよい。要は、暗号化手段30における暗号化の際に、暗号鍵変更タイミングがIピクチャの途中とならないよう暗号鍵変更タイミングを遅延させることができればよいのであり、それを可能とするものであれば他の任意の手法を用いるようにしてもよい。

[0072] また、本実施例1においては、1つのIピクチャを複数の暗号鍵で暗号化しないようにしたが、複数の暗号鍵で暗号化しないようにする領域は1つのIピクチャに限られず、例えば1つのIピクチャに加えて1つのPピクチャまたはBピクチャも含むような領域としてもよい。また、本実施例1においては、暗号化の方式としてCBCを用いることとしたが、暗号化の方式はCBCに限られるものではない。

[0073] なお、CBCブロックのサイズと記録媒体50の物理的なアクセスサイズとをマッチングさせ、またコンテンツへのアクセス開始位置とCBCブロックの開始位置とをマッチングさせるようにしたほうが望ましい。すなわち、物理アクセス単位が512バイトであって、論理的にその倍数、例えば6144バイト単位にしかアクセス出来ない場合は、CBCブロックサイズを、このアクセス単位にマッチングさせる。また、コンテンツへのアクセスは、該当アクセス位置を含む記録メディアのセクタの先頭から行われるので、アクセス開始位置とCBCブロックの開始位置とをマッチングさせておけば、セクタへのアクセスと同時にCBCブロックに対してアクセスできることになり、復号化の処理を簡略化することが可能となる。

[0074] [実施例2]

図6ー8に従って実施例2について説明する。図6は、本発明の実施例2にかかる暗号化記録装置の構成を説明するためのブロック図である。なお、図6に示す各構成要素のうち、図1に示す実施例1の各構成要素と同一の機能を達成する構成要素には同一番号を付している。本実施例2においては、1つのGOPが複数の復号鍵で復

号されることがないよう、1つのGOPは1つの暗号鍵で暗号化する。

[0075] 前述したように、Iピクチャ、PピクチャおよびBピクチャの組み合わせによってGOP(Group of picture)が構成される。また、1つのGOPには、少なくとも1つのIピクチャが必ず含まれている。

[0076] この暗号化記録装置15は、オーサリング処理機能を有しており、情報供給手段20、暗号化処理手段100、記録手段40、CPU60および記憶手段62を備えている。暗号化処理手段100は、暗号化手段30および鍵生成手段32を備えている。また、暗号化記録装置15は、記録媒体50と接続されている。オーサリング処理は非リアルタイム処理であるため、入力されるパーシャルTS信号のエンコード後のサイズを予め知ることができ、また鍵変更位置も自由に決定することができる。

[0077] 情報供給手段20には、例えば、外部の記憶装置などからパーシャルTS信号などの符号化された映像データが入力される。パーシャルTS信号は、シーケンスヘッダコード(SHC)、データ長が不定長の複数のGOPなどから構成されている。すなわち、GOPを含むデータ列の長さは、MPEGのエンコード方式や画素数などによって変化する。情報供給手段20は、CPU60からの制御信号によって動作の開始や停止が制御されており、外部入力されるパーシャルTS(Transport Stream)信号を、暗号化手段30において暗号化されるデータサイズ毎にバッファリングしながら所定のタイミングで暗号化手段30に供給する。

[0078] また、情報供給手段20は、暗号化手段30で行われる暗号化処理の際の鍵変更位置(鍵変更タイミング)に関する情報をCPU60から取得するとともに、入力されたパーシャルTS信号における隣接するGOP間の区切り位置を検出する。そして、情報供給手段20は、鍵変更位置とGOP間の区切り位置が一致するか否かを判定し、不一致の場合は、GOPの直前に別言すればGOPの最後に意味のないデータ、すなわちNULLパケット、あるいはランダムデータを含んでいるプライベートパケットなどを付加する処理を実行することにより、暗号鍵変更タイミングがGOP(符号化単位)を暗号化する途中とならないようにする。

[0079] 暗号化処理手段100は、暗号化単位である暗号化ブロック(CBCブロック)の個数をカウントするCBC(Cipher Block Chaining)カウンタ31を備える暗号化手段30と、

CPU60からの鍵生成通知信号に従って、一定時間間隔あるいは一定のCBCブロック数毎に、順次異なる暗号鍵を生成する鍵生成手段32とを有している。暗号化手段30は、鍵生成手段32で生成された暗号鍵を用いて情報供給手段20から入力されるパーシャルTS信号に対し固定長の暗号化ブロック毎に暗号化を行うものであり、暗号化された暗号化データを記録手段40に出力する。

[0080] 記録手段40は、暗号化手段30から得た暗号化データと、CPU60から得た暗号化データの管理情報(記憶手段62に一時記憶される)を記録媒体50に記録させる。記録媒体50は、ハードディスク,DVDなどの光記録媒体等の記録メディアであり、記録媒体50には、記録手段40から送られる暗号化データおよび暗号化データの管理情報が記録される。

[0081] CPU60は、暗号化記録装置15の各構成要素(情報供給手段20、暗号化手段30、記録手段40)を統括的に制御するとともに、暗号化手段30で暗号化された暗号化データの管理情報を記憶手段62に一時的に記憶する。また、CPU60は、暗号鍵変更タイミング信号としての鍵生成通知信号を、例えば、所定個数のCBCブロック数に対応する一定時間間隔で、暗号化手段30に出力する。

[0082] 記憶手段62には、図2に示したように、鍵適用数Aと、鍵情報X、鍵適用開始CBC番号Yおよび鍵適用CBC数Zからなる鍵適用範囲情報B1ーBnが記憶される。また、記録媒体50には、図3に示したように、記録された暗号化データの管理情報ファイルと、暗号化手段30で暗号化された暗号化データが記録される。

[0083] つぎに、情報供給手段20で行われる、鍵変更タイミングとGOP間の区切り(GOPの先頭)を合わせる処理について、図7および図8を用いて説明する。

[0084] 図7は、CBCとGOPの関係を説明するための図である。図7において、暗号化を行うためのCBCブロックは固定長である。図7中、最初の複数のCBCブロック1(CBC1)は同一の第1の暗号鍵で暗号化が行われ、つぎの複数のCBCブロック2(CBC2)が第1の暗号鍵とは異なる第2の暗号鍵で暗号化が行われるように設定されている。すなわち、時点aが鍵変更タイミングである。

[0085] 一方、情報供給手段20に入力された初期段階でのパーシャルTS信号においては、1つのGOP(GOP1)とつぎのGOP(GOP2)との区切りが、時点(位置)cに存在し

ていたものとする。この場合、初期段階のパーシャルTS信号においては、鍵変更タイミングaは、GOP2の途中となり、GOP2は、第1の暗号鍵および第2の暗号鍵によって暗号化されてしまう。

[0086] そこで、実施例2においては、情報供給手段20が図8に示すような処理を行うことで、1つのGOPが1つの暗号鍵で暗号化されるようにしている。

[0087] まず、情報供給手段20は、CPU60からアライメント要求が入力されると、入力されたパーシャルTS信号における隣接するGOP間の区切り位置を検出するとともに、暗号化処理の際の鍵変更位置を検出する(ステップS510)。GOP間の区切り位置は、GOPヘッダ等によって検出することができる。CBCブロックは固定長であるので、鍵変更位置は、CPU60から、CBCブロック長(固定長)および同一鍵で暗号化を行うCBCブロック数などの鍵変更位置(鍵変更タイミング)に関する情報を得ることで、導出することができる。

[0088] 情報供給手段20は、取得したGOP間の区切り位置と、鍵変更位置とが一致するか否かを判定する(ステップS520)。この判定の結果、GOP間の区切り位置と鍵変更位置とが不一致の場合は、図7に示すように、鍵変更位置とGOP間の区切り位置(GOPの先頭位置)とが一致するように、GOP間に、別言すれば次のGOPの直前にNULLパケットを挿入する(ステップS530)。

[0089] 図7の場合は、GOP1とGOP2の間に、鍵変更位置aとGOP間の区切り位置とが一致するデータ長のNULLパケットが挿入されている。これによって、GOP2は、CBC2の暗号化用の鍵のみによって暗号化されることとなる。このように、1つのGOPが1つの暗号鍵で暗号化される場合は、1つのGOPを1つの復号鍵で復号化することが可能となる。

[0090] このように実施例2によれば、暗号鍵変更位置に対しGOPの先頭位置が一致するようにNULLパケットなどの意味のないデータを挿入しているので、受信したMPEG—TS等の符号化映像データをオーサリン処理する機能を有する暗号化記録装置において、1つのGOPが1つの暗号鍵で暗号化されることになり、早送り再生やサーチなどの特殊再生時にスムーズな映像表示が可能となる。

[0091] なお、上記実施例2においては、鍵変更位置とGOP間の区切り位置(GOPの先頭

位置)とを検出し、これらが一致するようにGOP間にNULLパケットを挿入するようにしたが、つぎのような実施も可能である。

[0092] すなわち、まず、情報供給手段20では、入力されたパーシャルTS信号中の全てのGOPのデータ長を検出する。そして、検出した各GOPのデータ長がCBCブロックのデータ長(固定長)の整数倍であるか否かを判定する。そして、そのデータ長がCBCブロックのデータ長の整数倍でないGOPに関しては、そのデータ長がCBCブロックのデータ長の整数倍となるように、そのGOPの最後にNULLパケットを挿入する。すなわち、この場合は、GOPの先頭がCBCブロックの区切りと一致するように、直前のGOPの末尾にNULLパケットを挿入する。そして、少なくも1つのGOPについては、同一の鍵で暗号化されるように鍵変更位置を適宜変更する。このようにすることにより、少なくとも1つのGOPを必ず1つの暗号鍵で暗号化することができる。

[0093] また、実施例2において、情報供給手段20で行った上記の処理を暗号化処理手段100で行わせるようにしてもよい。

請求の範囲

[1] フレーム内符号化画像を少なくとも含む符号化単位により構成される符号化データが入力される入力手段と、

前記符号化データを所定の暗号化単位で暗号化するとともに、一又は複数の暗号化単位毎に暗号鍵を変更しつつ前記符号化データを暗号化する暗号化処理手段と、

前記暗号化された符号化データを記録媒体に記録する記録手段とを備えた暗号化記録装置において、

前記暗号化処理手段は前記一つのフレーム内符号化画像を暗号化する途中で暗号鍵が変更されないよう少なくとも一つのフレーム内符号化画像を単一の暗号化鍵で暗号化すること、

を特徴とする暗号化記録装置。

[2] 前記暗号化処理手段は、暗号鍵変更タイミングが前記フレーム内符号化画像を暗号化する途中となる場合は、前記フレーム内符号化画像を暗号化する途中に暗号鍵が変更されないよう前記暗号鍵変更タイミングを遅延させることを特徴とする請求項1に記載の暗号化記録装置。

[3] 前記入力手段は、入力された符号化データ中からフレーム内符号化画像を検出し、フレーム内符号化画像の検出に応じて識別フラグの状態を変化させるデータ識別手段を有し、 前記暗号化処理手段は、前記識別フラグの状態に基づいて暗号鍵変更タイミングを遅延させるか否かを判断することを特徴とする請求項2に記載の暗号化記録装置。

[4] 前記データ識別手段は、フレーム内符号化画像の先頭を検出した時点から前記フレーム内符号化画像とは異なる符号化画像の先頭を検出した時点までの期間、前記識別フラグを、暗号鍵の変更を禁止する状態とすることを特徴とする請求項3に記載の暗号化記録装置。

[5] 前記入力手段は、暗号鍵変更タイミングが前記符号化単位を暗号化する途中となる場合は、前記符号化単位を暗号化する途中で暗号鍵が変更されないように符号化単位の直前に意味を持たない情報を挿入することを特徴とする請求項1に記載の暗

号化記録装置。

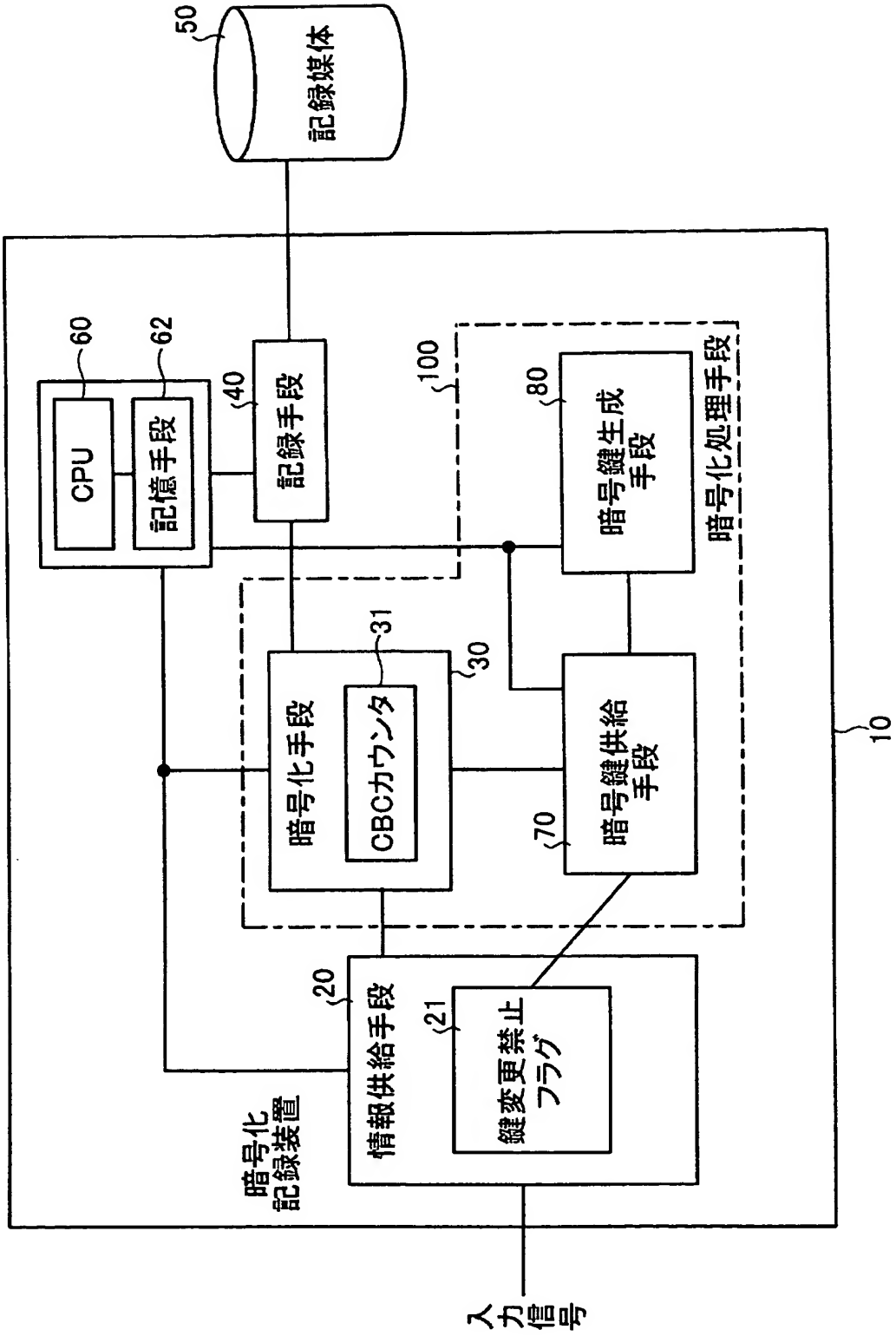
[6] フレーム内符号化画像を少なくとも含む符号化単位により構成される符号化データを、暗号鍵を変更しながら所定の暗号化単位で暗号化して記録する暗号化記録方法において、 前記一つのフレーム内符号化画像を暗号化する途中で暗号鍵が変更されないよう少なくとも一つのフレーム内符号化画像を単一の暗号化鍵で暗号化することを特徴とする暗号化記録方法。

[7] 暗号鍵変更タイミングが前記フレーム内符号化画像を暗号化する途中となる場合は、前記フレーム内符号化画像を暗号化する途中に暗号鍵が変更されないよう前記暗号鍵変更タイミングを遅延させることを特徴とする請求項6に記載の暗号化記録方法。

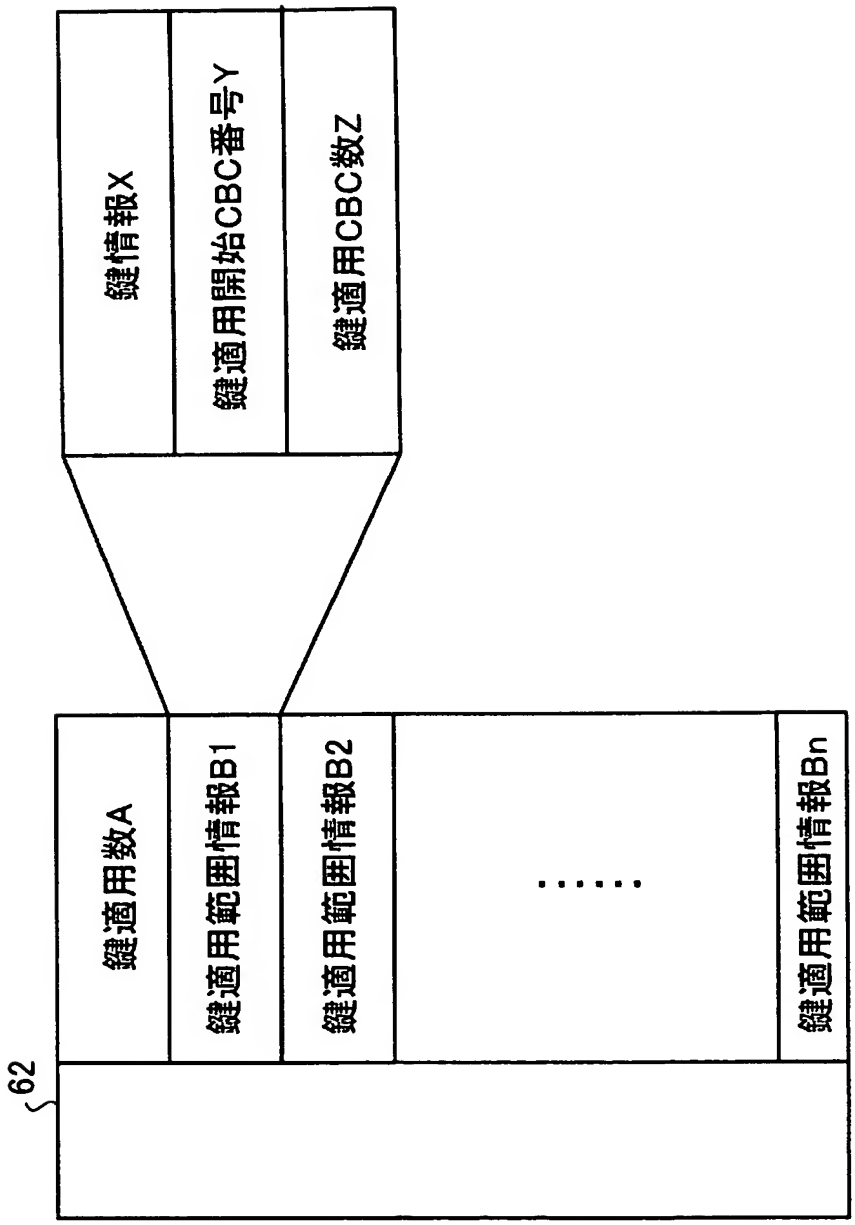
[8] 暗号鍵変更タイミングが前記符号単位を暗号化する途中となる場合は、前記符号化単位を暗号化する途中で暗号鍵が変更されないように符号化単位の直前に意味を持たない情報を挿入することを特徴とする請求項6に記載の暗号化記録方法。

WO 2005/043806 PCT/JP2004/016149

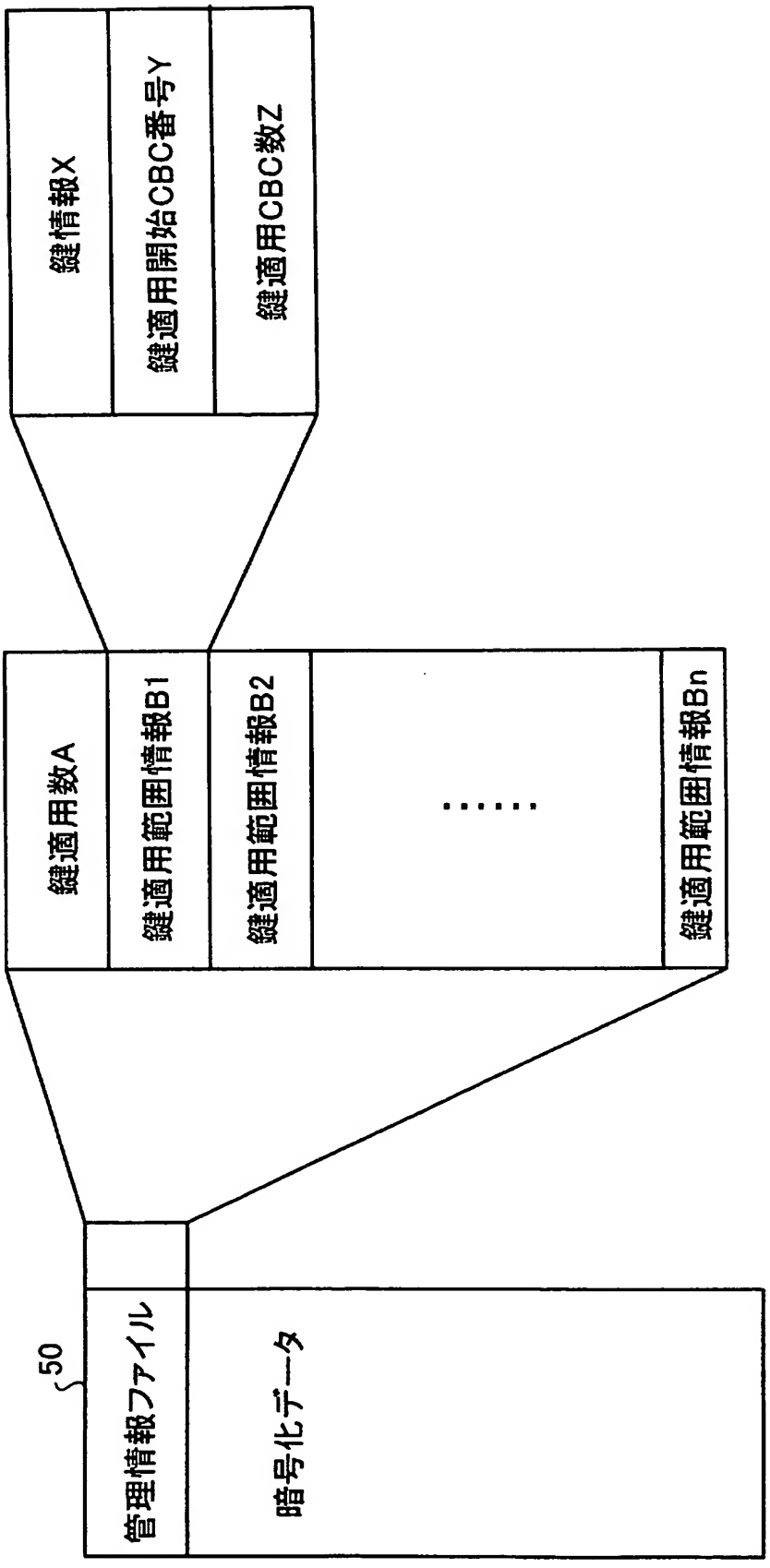
[図1]



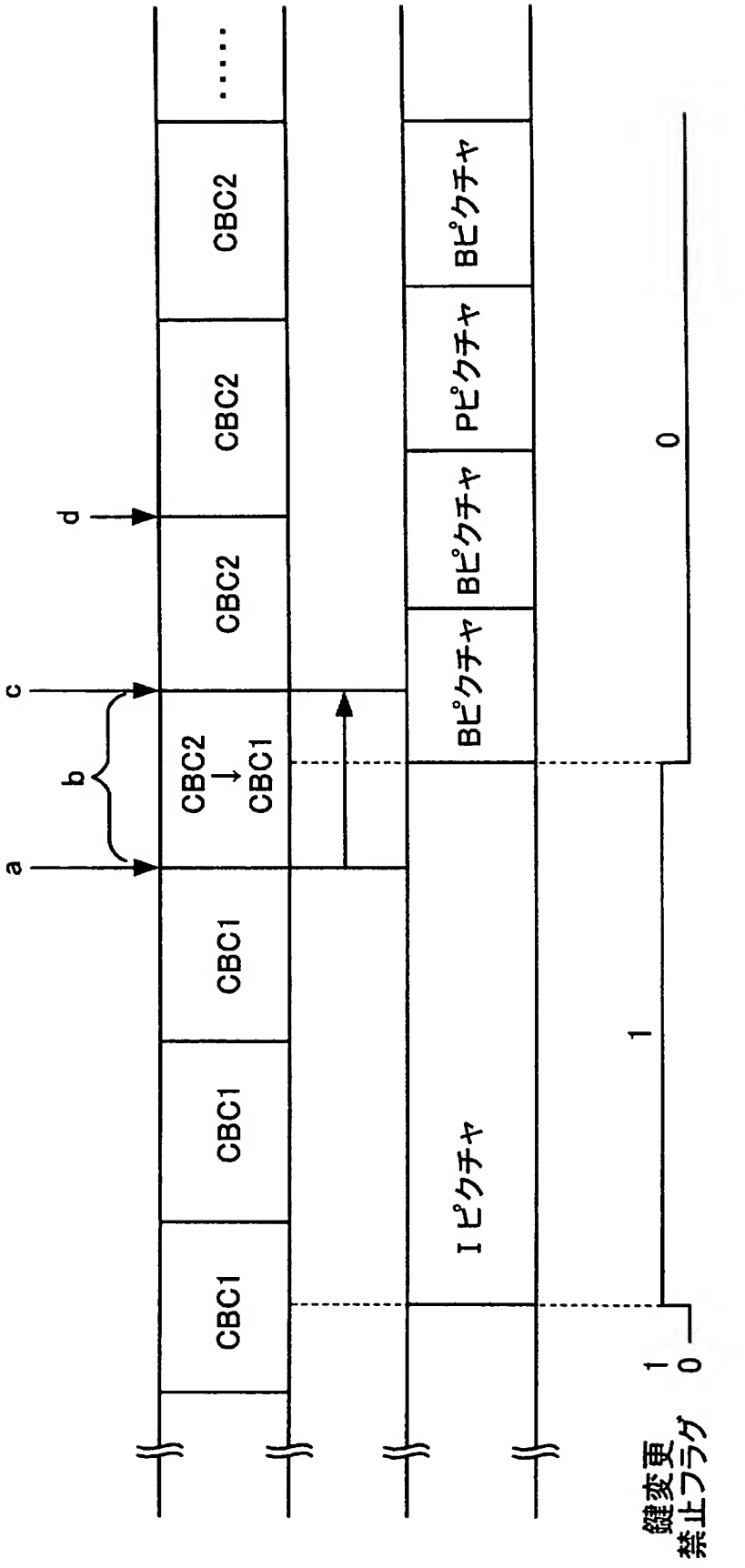
[図2]


鍵情報X
鍵適用開始CBC番号Y
鍵適用CBC数Z
鍵適用数A
鍵適用範囲情報B1
鍵適用範囲情報B2
.....
鍵適用範囲情報Bn
62

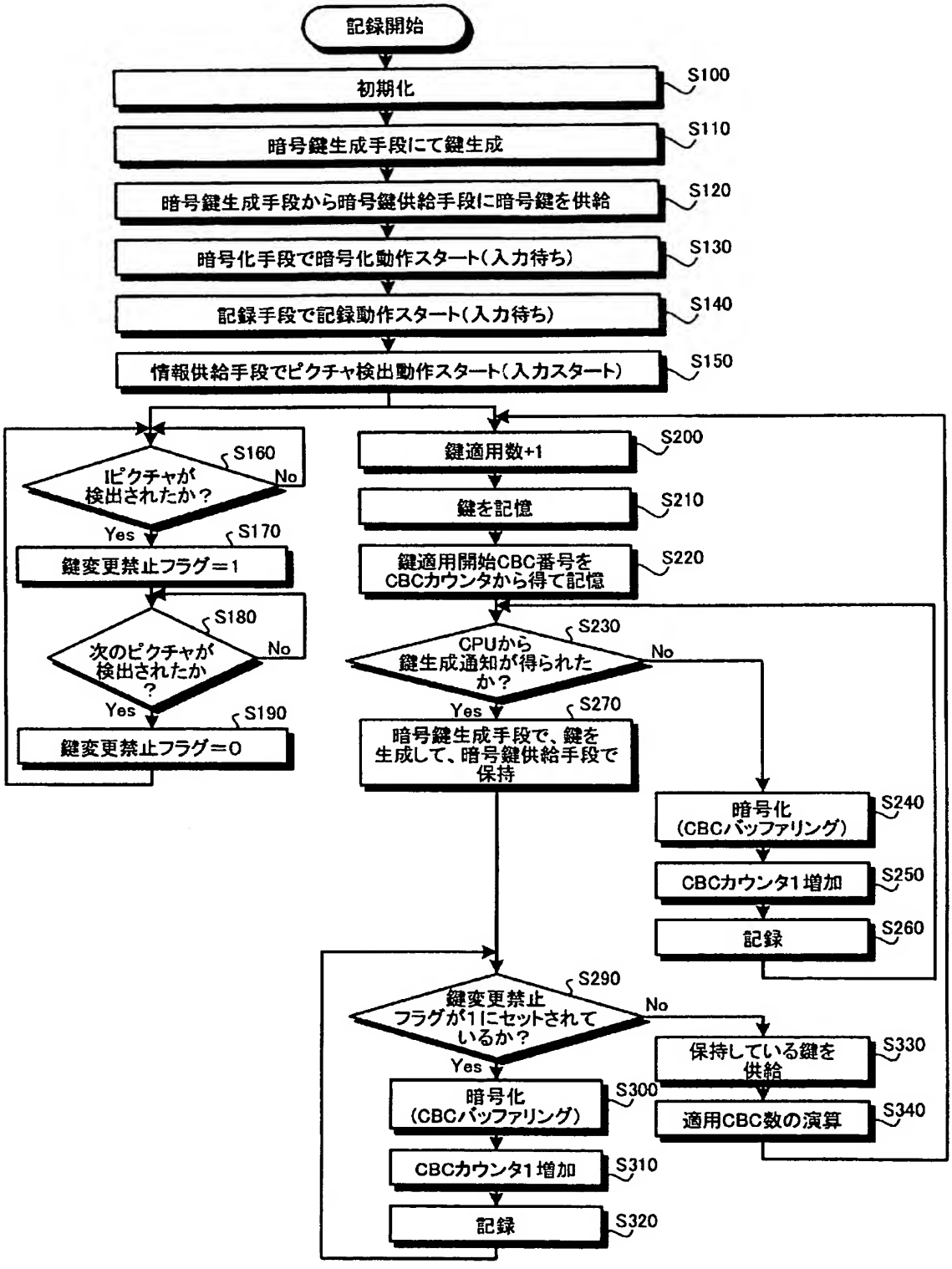
[図3]


50
管理情報ファイル
暗号化データ
鍵適用数A
鍵適用範囲情報B1
鍵適用範囲情報B2
.....
鍵適用範囲情報Bn
鍵情報X
鍵適用開始CBC番号Y
鍵適用CBC数Z

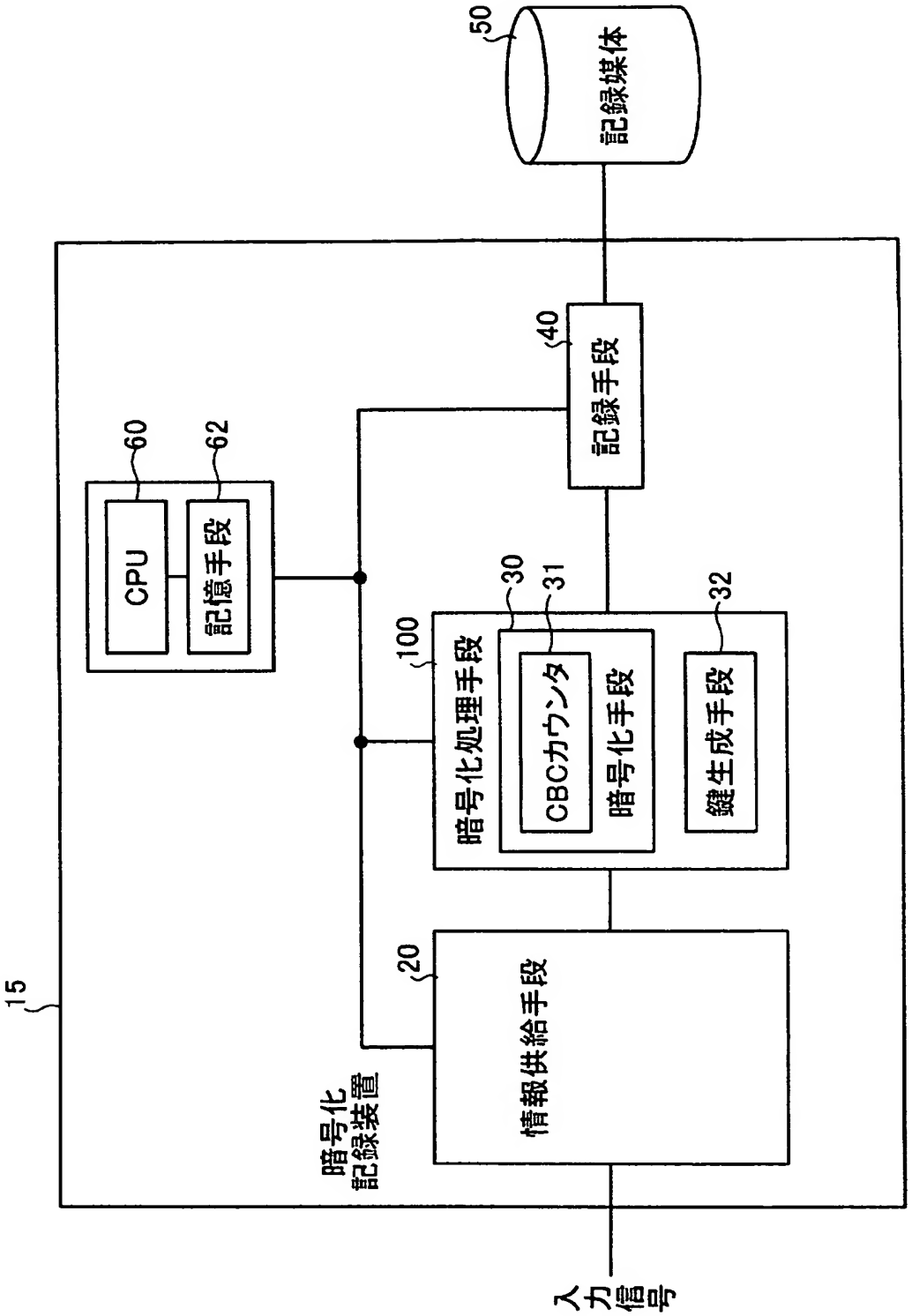
[図4]


CBC1
CBC1
CBC1
CBC1
CBC2
CBC2
CBC2
CBC2
.....
a
b
c
d
CBC2
↓
CBC1
Iピクチャ
Bピクチャ
Bピクチャ
Bピクチャ
Pピクチャ
Bピクチャ
0
1
鍵変更
禁止フラグ
1
0

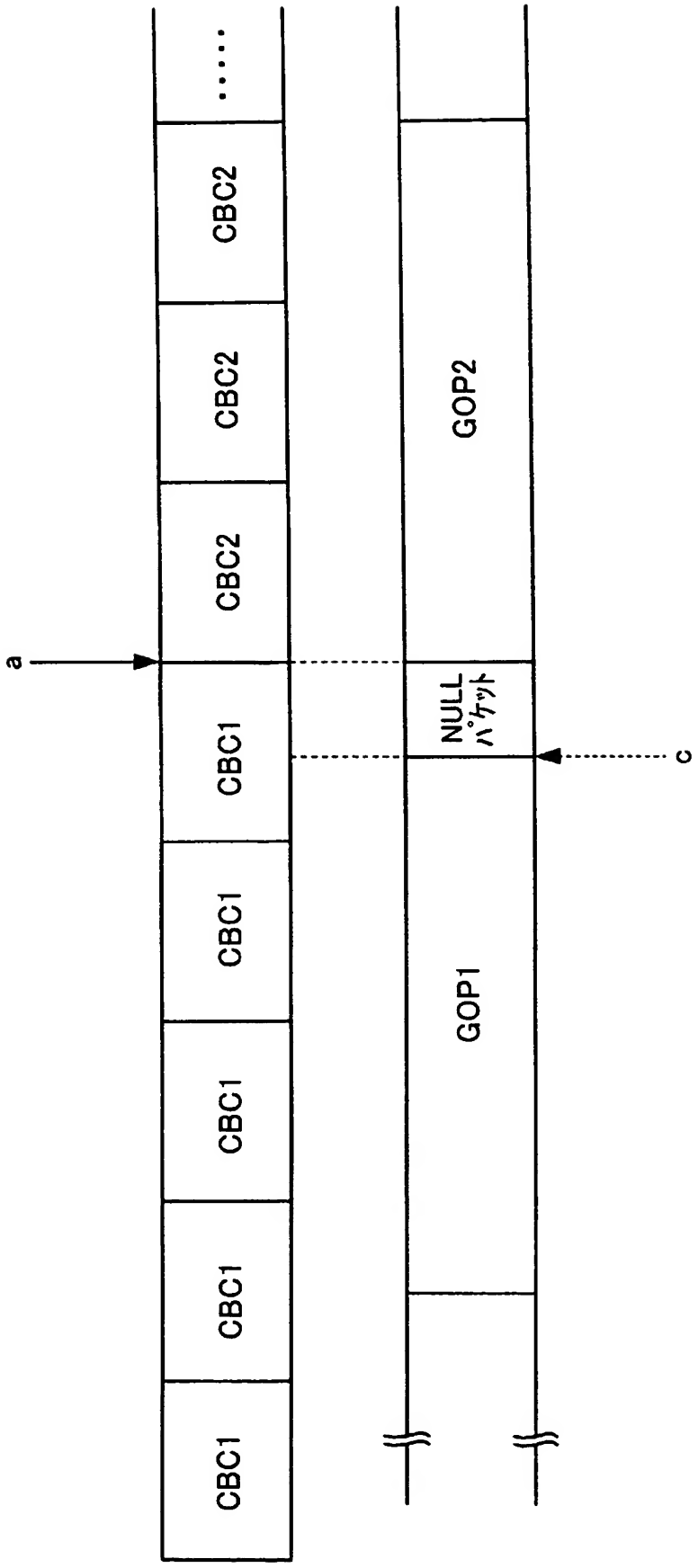
[図5]


記録開始
初期化
S100
暗号鍵生成手段にて鍵生成
S110
暗号鍵生成手段から暗号鍵供給手段に暗号鍵を供給
S120
暗号化手段で暗号化動作スタート(入力待ち)
S130
記録手段で記録動作スタート(入力待ち)
S140
情報供給手段でピクチャ検出動作スタート(入力スタート)
S150
Iピクチャが検出されたか？
S160
No
Yes
鍵変更禁止フラグ＝1
S170
次のピクチャが検出されたか？
S180
No
Yes
鍵変更禁止フラグ＝0
S190
鍵適用数+1
S200
鍵を記憶
S210
鍵適用開始CBC番号をCBCカウンタから得て記憶
S220
CPUから鍵生成通知が得られたか？
S230
No
Yes
暗号鍵生成手段で、鍵を生成して、暗号鍵供給手段で保持
S270
暗号化(CBCバッファリング)
S240
CBCカウンタ1増加
S250
記録
S260
鍵変更禁止フラグが1にセットされているか？
S290
No
Yes
保持している鍵を供給
S330
暗号化(CBCバッファリング)
S300
適用CBC数の演算
S340
CBCカウンタ1増加
S310
記録
S320

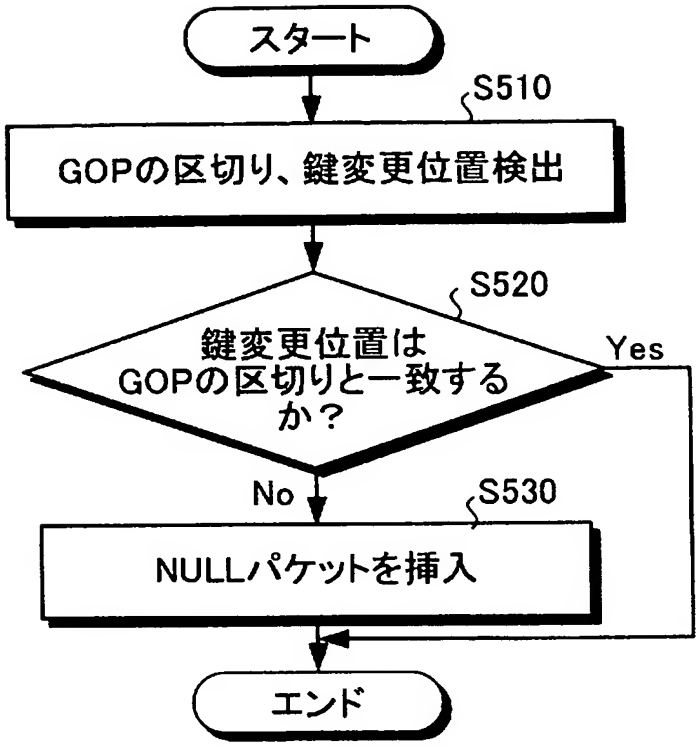
[図6]


50
記録媒体
40
記録手段
60
62
CPU
記憶手段
30
31
32
100
暗号化処理手段
CBCカウンタ
暗号化手段
鍵生成手段
20
情報供給手段
15
暗号化
記録装置
入力信号

[図7]


CBC2
CBC2
CBC2
CBC1
CBC1
CBC1
CBC1
CBC1
GOP2
GOP1
NULL パケット
a
c

[図8]


スタート
S510
GOPの区切り、鍵変更位置検出
S520
鍵変更位置は
GOPの区切りと一致する
か？
Yes
No
S530
NULLパケットを挿入
エンド

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/016149

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/14, H04L9/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/14, H04L9/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2003-46973 A (Nippon Hoso Kyokai), 14 February, 2003 (14.02.03), Par. Nos. [0050], [0070] to [0085]; Fig. 4 (Family: none)	1,6 2-5,7,8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 November, 2004 (15.11.04)	30 November, 2004 (30.11.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号 PCT／JP2004／016149

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9／14, H04L9／16

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9／14, H04L9／16

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2003-46973 A（日本放送協会）2003.02.14, 段落【0050】, 【0070】－【0085】, 図4（ファミリーなし）	1, 6
A		2-5, 7, 8

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 15. 11. 2004	国際調査報告の発送日 30.11.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里 裕正 5M 3365 電話番号 03－3581－1101 内線 3597

様式PCT／ISA／210（第2ページ）（2004年1月）